



A trusted storage and data retrieval in cloud computing

Shyamala MG^{1✉}, Narmada B², Nivetha SM²

1. Faculty, Department of Electronics and Communication Engineering, Dhirajlal Gandhi College of Technology, Salem, TamilNadu 636309, India
2. Faculty, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, TamilNadu 636309, India

✉**Corresponding Author:** Faculty, Department of Electronics and Communication Engineering, Dhirajlal Gandhi College of Technology, Salem, TamilNadu 636309, India; Email – shyamala.ajays@gmail.com

Publication History

Received: 09 June 2015

Accepted: 13 July 2015

Published: 1 August 2015

Citation


Shyamala MG, Narmada B, Nivetha SM. A Trusted Storage and Data Retrieval in Cloud Computing. Discovery, 2015, 34(154), 43-47

Publication License



© The Author(s) 2015. Open Access. This article is licensed under a [Creative Commons Attribution License 4.0 \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/).

General Note

 Article is recommended to print as color digital version in recycled paper.

ABSTRACT

Data storage in cloud provides is a least cost method for the small, medium and large enterprises across the world. But the main issue for the wide spread adoption of cloud storage is the lake of security in the technology used for storage and retrieval by its user. The data which is to be stored on multiple servers and the location is concealed from the customers and they have no more in control of the data. This significant feature of the cloud storage provides many security and trust challenges. The main disadvantage is decryption ciphers is not identical to the original data. In this paper we propose a trusted architecture of data storage and retrieval in cloud. The architecture presents a unique way of secured storage and accessing of data from the cloud data centre. It also ensures that only the user who is authorized will be able to access the stored data and decrypt. Additionally, if there is any violation of the security parameter at the data centre where the data is stored, the data will still be secured i.e. the data will be stored in encrypted form and any time the data can be retrieved by the user using inverse cipher text.

Keywords: Security Challenges, Trusted Storage, Access Control, Secured storage, Cloud Computing.

1. INTRODUCTION

Many architecture of information system is presented in the recent past in the name of cloud computing, which is seen to be a revolution in the history of cloud computing industry. This computing paradigm offers a unique structure of the utilization of computing resources to business, institutions and individual users by cloud servers as alternative to their own computing infrastructure [YBD 08] [UXU 12]. The customers are not only provided the advantage from the requirement of costly hardware equipment by Cloud Computing, rather it has reduced the complexity for their requirement from customer point of view. Cloud computing provides user the illusion of unlimited computing resources. The user can acquire computing resources as required, or as nanoscopic as they required, irrespective of the maintenance and provision of those available resources [UXF 12] [GRO 09].

When considering the history of cloud computing, it is regularly found with data disclosures either premeditated or unpremeditated. This discloses the risks of privacy and confidentiality of the cloud data storage and retrieval deployment. The first risk is the unexpected disclosure of data which occurs because of the errors in the design of the cloud computing software of the cloud providers. For example, the non-authenticated users are allowed to avail the documents by Google Docs due to a bug [KIN 09], whereas the Flickr and Face book have also not secured the private pictures of their users due to flaws.

Usually all the cloud computing data centres have a central server administration system, which is responsible for the management of overall operations of the provided data centres. Cloud computing provides storage in a centralized manner, processing memory, and bandwidth. Due the centralization of computing resources, it is an attractive target for inside or outside attackers.

The cloud data service provider's record of user's data is not secured in cloud storage. In reality, Twitter has made an agreement with Federal Trade commission of the United States due to its unsystematic security practices allows the attackers to dissimulate as any authorize user of the system in 2011 [FTC 11]. In addition, several such sites have undergone occurrences of security lapses which results in the data loss of cloud users which not only include email addresses but credit card pin numbers and related data's as well [MIL 11].

Cloud data service providers faces more pressure from government agencies. Google Inc. obeys with most of the requests it receives and it provides the private data of its clients to such requests. Additionally, all the government agencies of several countries have threatened to block the blackberry email services if they are not given the permission to monitor the users' private data [REA 10].

Most of the time, the cloud services providers frequently encompass some money-making inducement from different private parties and thus willingly distribute the users' private data, which the users think is private and secured. Google and Face book are the service providers which have destabilized their policy and default settings of privacy in order to endorse new products and their services. Moreover, the cloud service provider keeps their promise still the data is safe [UXF 13] [VIJ 12]. Users have a worry about data confidentiality, security and unauthorized access to the data [UXF 13]. This problem becomes worse in the case of cloud computing as the user do not have knowledge about the physical location of the data and control over the data centre to which they are concerned. A mischievous data service provider can possibly damage the data of the users by updating, plummeting and transforming.

Trust in the cloud is mainly based on the security of their data which is offered by the service provider. It is a known fact that if the system is secured, then it should be trustworthy [STO 10] [UXF 13]. In this paper a trusted architecture for data storage and data retrieval in cloud computing which would focus the security of cloud computing environment is proposed. The cloud data architecture is generally composed of three entities the cloud servers, the media and the clients. Major of the research work is done on securing the server but no importance is given to the channel of transfer between the client and the cloud. An alternative architecture is proposed in this paper which covers all the aspect. i.e., access control, data transfer through the channel and finally data storage and retrieval from the cloud computing data storage. This will results, enhancing trust on cloud computing.

2. RELATED WORK

A hopeful computing environment was proposed by researchers for cloud computing in 2010 which provides the protection of data via strong authentication mechanism, and restricted access by role based access control method in cloud computing system [STO 10]. The previous works are based on providing trusted storage architecture for cloud computing and security. It is found that numerous systems and methods are incorporated to secure the cloud from different perspective in which some of the systems work to develop a trusted cloud environment by providing high level of security.

There are diverse models that divide and store the user data on different cloud providers as alternative to a single storage service provider. A multi – clouds database model is an alternative to single cloud environment [UXF 11]. The purpose of this model was to preserve the cloud system from the threat of malicious insider and thwart the failure of the cloud services infrastructure.

A novel architecture for authenticated key exchange utilizes the internet key exchange and randomness reuse approach [LZC 11]. A Trust management model was introduced by TFMC for cloud computing which is based on the fuzzy set theory [SCL 11]. Here the user can use this in decision making during the selection of a specific cloud service provider so that trustworthiness can be analyzed for different cloud service providers. It also provides trust relationship among multiple cloud providers.

Y. Singh et.al., [SKZ 11] proposed a unique cost effective and secure model of data distribution for multi – cloud storage. This model provides a low cost mechanism of user's data distribution of on available multiple cloud storage providers. The single sign on (SSO) is implemented on the top layer of the cloud computing model. The justification to this mechanism was to present the user with the best quality of service through secure storage and availability of data [UXF 13] [ABH 11]. This method minimizes the number of login and enhances the security of the overall system. A public auditing architecture for cloud computing has been developed for privacy preserving and public audit ability [ZZY 11] [UXF 13] [QWL 09] [CRL 10]. This architecture not only provide the privacy preservation but also support block less verification, public audit ability dynamic operation support on data, etc. These architectures are proved to be insecure due to its incapability to stand against the existential forgery by a known message attack [CXD 12]. The authors proposed a protocol for dynamic data auditing which poses a disadvantage that the data may be disclosed to the auditor as the server sends the linear blocks of data to them. Several works of this kind are enduring different kind of security issues. Some cannot thwart the illicit data access by the cloud service provider while some face the problem of insider spiteful activity. Many mechanisms are expensive in terms of finances, requirement of a time for data processing and the availability of affected data. To avoid such disadvantages a model was proposed that allow only the lawful user to access and store data with confidence. This scheme provide security of data at rest ie., stock up of data at server and also provides protection during the transmission at transmission media. The disadvantage in this is that the retrieval of the original content via decryption is not guaranteed. An architecture recommended in this paper espouses different algorithms for encryption and decryption.

3. THE PROPOSED ARCHITECTURE

The proposed architecture is composed of two modules, i.e. the client module and the cloud module. The general description of the model is given below.

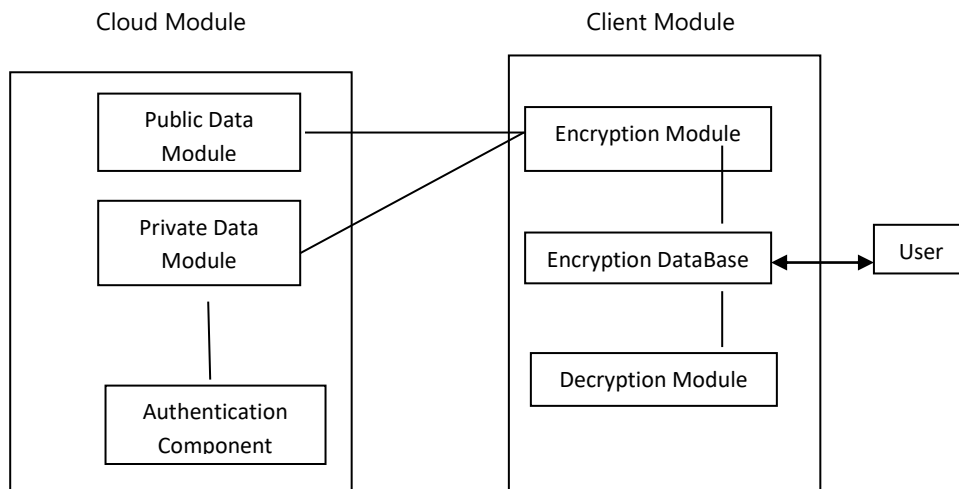


Figure 1 Proposed architecture for data storage and retrieval in cloud

3.1. The Client Module

The client module is composed of three components.

- Encryption Component
- Encryption Database
- Decryption Component

3.1.1. Encryption Component

The private/public data is sent to encryption component. The encryption component applies the AES encryption techniques and sends the encrypted data to Encryption Database storage, where the data is stored in the public component of the data storage

server. The key will be store in the private data component. The key is taken from the private data component and data from the public data component for decrypting the data

3.1.2. Encryption Database

The encrypted data from the encryption component is passed onto the encryption database which acts as a secured storage. When the user requires the original data, the data from the database is moved to the decryption component. This in turn uses key from the private data module.

3.1.3. Decryption Component

Usually decryption is done to extract the original text from the encrypted cipher text. But using AES, decryption ciphers is not identical to the original data .So we use inverse cipher text to retrieve the original data.

3.2. The Cloud Module

The cloud server module also composes three components namely,

- Public data component.
- Private data component
- Authentication component

3.2.1. Public Data Component

The data stored in the public component will be shared among all the authorized users of that data. All these data stored in the public data component will be transformed to an encrypted form. Along with the creation of data in this component the owner is responsible also for the different data operations as well.

3.2.2. Private Data Component

The private data component is responsible for the storage of the user's information such as Login data and also for the storage of secrete keys that are required for the decryption of the data in the public data component. Only the owner of the data can access the private data section of the storage. They can perform functions on data such as delete, append, update. Added to this the performance of such operations on private data component is not endorsed for users.

3.2.3. Authentication Component

The authentication component works in association with the private data component. When the server receives a request from the authorized user for data access, it is the duty of authentication module to arbitrarily generate a two session password. It sends one of it to user's email and the other to their mobile number. The user is then legitimated via the session passwords from the user.

4. SECURITY ANALYSIS OF THE PROPOSED ARCHITECTURE

The proposed architecture is very simple and highly secure. The access of data is controlled by implementing a multi-level authentication mechanism [UXF 13]. Apart from accessibility, the data is provided with multiple level of security by the encryption process which also makes it more secure. We know that there are a lot of cryptographic algorithms which are contemplate to be very efficient at algorithmic level. In our proposed architecture we use AES algorithm for encryption of data files. The overall performance of this scheme is best when considering both the software and hardware implementation. The algorithm is simple, fast and compact [GCF 11] [DKA 06] [NJA 05] [SMA 11]. The encrypted cipher text is stored in database and Decrypted by decrypting algorithm. Inverse cipher text is available through which the stored encrypted data can be retrieved which is identical to the original data.

5. CONCLUSION

The users are getting attracted towards cloud technology nowadays. A trusted architecture for data storage and retrieval is presented for cloud computing environment. It not only provides secured access of data but also provides a trusted mechanism for data transmission through a channel and retrieval of data from encrypted database. The architecture stops the unauthorized user from accessing data before it is encrypted by the encryption algorithm. The proposed architecture increases the level of confidentiality and integrity of the stored and retrieved data.

REFERENCE

1. [ABH 11] R. G. Ashish and D. M. Bhavsar, "Securing user authentication using single sign-on in Cloud Computing", IEEE Nirma University International Conference on Engineering (NUICONe), (2011), pp. 1-4.
2. [CRL 10] W. Cong, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services", IEEE Network, vol. 24, no. 4, (2010), pp. 19-24.
3. [CXD 12] X. U. Chun-xiang, H. E. Xiao-hu and A. Daniel, "Cryptanalysis of auditing protocol proposed by Wang, et al., for data storage security in Cloud Computing", (2012).
4. [DKA 06] M. -Z. Dawood, A. R. Khan and S. Akhter, "Advance Encryption Standard", The 18th Saudi National Computer Conference (NCC18), (2006), pp. 01 – 13.
5. [FTC 11] U.S. Federal Trade Commission, FTC accepts final settlement with twitter for Failure to safeguard personal information, (2011) March, <http://www.ftc.gov/opa/2011/03/twitter.shtm>.
6. [GCF 11] S. Guha, B. Cheng and P. Francis, "Privat: Practical privacy in online advertising", 8th USENIX Symposium on Networked Systems Design and Implementation (NSDI), (2011), pp. 1 – 14.
7. [GRO 09] R. L. Grossman, "The Case for Cloud Computing", IT Professional, vol. 11, no. 2, (2009), pp. 23 – 27.
8. [KIN 09] J. Kincaid, "Google privacy blunder shares your docs without permission", TechCrunch, (2009) March, <http://techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/>.
9. [LZC 11] E. C. Liu, X. Zhang, J. Chen and C. Yang, "An Authenticated Key Exchange Scheme for Efficient Security Aware Scheduling of Scientific Applications in Cloud Computing", IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), (2011), pp. 372 – 379.
10. [MIL 11] E. Mills, "Hackers release credit card, other data from stratfor breach", CNET News,(2011) December, http://news.cnet.com/8301-27080_3-57350361-245/hackers-release-credit-card-other-data-from-stratfor-breach/.
11. [NJA 05] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms", IEEE First International Conference on Information and Communication Technologies, (ICICT 2005), pp. 84-89.
12. [REA 10] M. Reardon, "India threatens to shut down blackberry service", CNET News, (2010) August, http://news.cnet.com/8301-30686_3-20012981-266.html.
13. [SCL 11] X. Sun, G. Chang and F. Li, "A Trust Management Model to Enhance Security of Cloud Computing Environments", International Conference on Networking and Distributed Computing, (2011), pp. 244 – 248.
14. [SKZ 11] Y. Singh, F. Kandah and W. Zhang, "A secured cost-effective multi-cloud storage in cloud computing", IEEE Computer Communications Workshops (INFOCOM WKSHPs), (2011), pp. 619 – 624.
15. [SMA 11] S. P. Singh and R. Maini, "Comparison of data encryption algorithms", International Journal of Computer Science and Communication, vol. 2, no. 1, (2011), pp. 125-127.
16. [STO 10] Z. Shena and Q. Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, (2010), pp. 11-15.
17. [QWL 09] W. Qian, C. Wang, J. Li, K. Ren and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", Computer Security–ESORICS (2009), pp. 355-370.
18. [UXF 11] A. M. Abdullatif, B. Soh and E. Pardede, "MCDB: Using Multi-clouds to Ensure Security in Cloud Computing", IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), (2011), pp. 784-791.
19. [UXF 12] S. Ullah, Z. Xuefeng, Z. Feng and Zhao Haichun, "TCLLOUD: Challenges and Best Practices for Cloud Computing", International Journal of Engineering Research and Technology, vol. 1, no. 9, (2012), pp. 01-05.
20. [UXF 13] S. Ullah, Z. Xuefeng and Z. Feng, "TCLLOUD: A Multifactor Access Control Framework for Cloud Computing", International Journal of Security and Its Applications, vol. 7, no. 2, (2013), pp. 15-26.
21. [UXF 13] S. Ullah, Z. Xuefeng and Z. Feng, "TCLLOUD: A Reliable Data Storage Architecture for Cloud Computing", Advanced Material Research, vol. 717, no. 2, (2013), pp. 677-687.
22. [UXF 13] S. Ullah, Z. Xuefeng and Z. Feng, "TCLLOUD: A New Model of Data Storage Providing Public Verifiability and Dynamic Data Recovery for Cloud Computing", Journal of Software Engineering and Applications, vol. 6, no. 3B, (2013), pp. 23-28.
23. [UXF 13] S. Ullah, Z. Xuefeng and Z. Feng, "TCLLOUD: Inter – Node Communication Model Based on Social Trust Framework for Cloud Computing", Advanced Material Research , vol. 717, no. 2, (2013), pp. 688-695.
24. [UXU 12] S. Ullah and Z. Xuefeng, "Cloud Computing: a Prologue", International Journal of Advanced Research in Computer and Communication Engineering, vol.1,no.1, (2012),pp.1 – 4.
25. [VIJ 12] J. Vijayan, "36 state AGs blast Google's privacy policy change" Computerworld, (2012) February, <http://www.pcadvisor.co.uk/news/mobile-phone/3340102/36-state-ags-blast-googles-privacy-policy-change/>.
26. [YBD 08] L. Yousef, M. Butrico and D. Da Silva, "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, (2008), GCE '08, pp. 1 – 10.
27. [ZZY 11] H. Zhuo, S. Zhong and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability", IEEE transactions on Knowledge and Data Engineering, vol. 23, no. 9, (2011), pp. 1432-1437.